Network Security

Best Practices for Mac OS X

Session 622

Network Security

Best Practices for Mac OS X

Definition

- Network security:
  - Protection of networks and their services from unauthorized modification, destruction, or disclosure

Security Focus

- Communication and data security
- Control access to system and services
- Management of access

Apple Design Philosophy

- Security at the core
- Conservative approach
- Open Source
- Open Standards
- Easy to use and configure
- Easy to manage

Security at the Core

- Open Source UNIX-based operating system
  - Password-protected logins
  - Security services built-in
  - UNIX file-level permissions
  - Home directories segregated from other users
  - Creation of multiple accounts
  - Protected Memory

Conservative Approach

- Secure default configurations:
- All services off by default
- Disabled root account
- Closed ports
- SSH vs Telnet

True Security?

“The only secure computer is one that is turned off, locked in a safe, and buried 20 feet down in a secret location –and I'm not completely confident of that one either.”

Bruce Schneier, principal of Counterpane Internet Security Inc.

Physical Security

- Protecting desktops and portables
  - Lock desktop case
  - Prevent memory theft
  - Protect firmware settings
  - Security cable

Protecting Server

- Protect your deployment and assets
  - Lock on enclosure
    for hardware and software security
  - Enclosure monitoring
    and intrusion alert

Open Firmware Security

- System startup protection
  - Control over how the system is booted
  - Easy to configure with GUI interface
  - Superset of IEEE 1275

Foundation Security Services

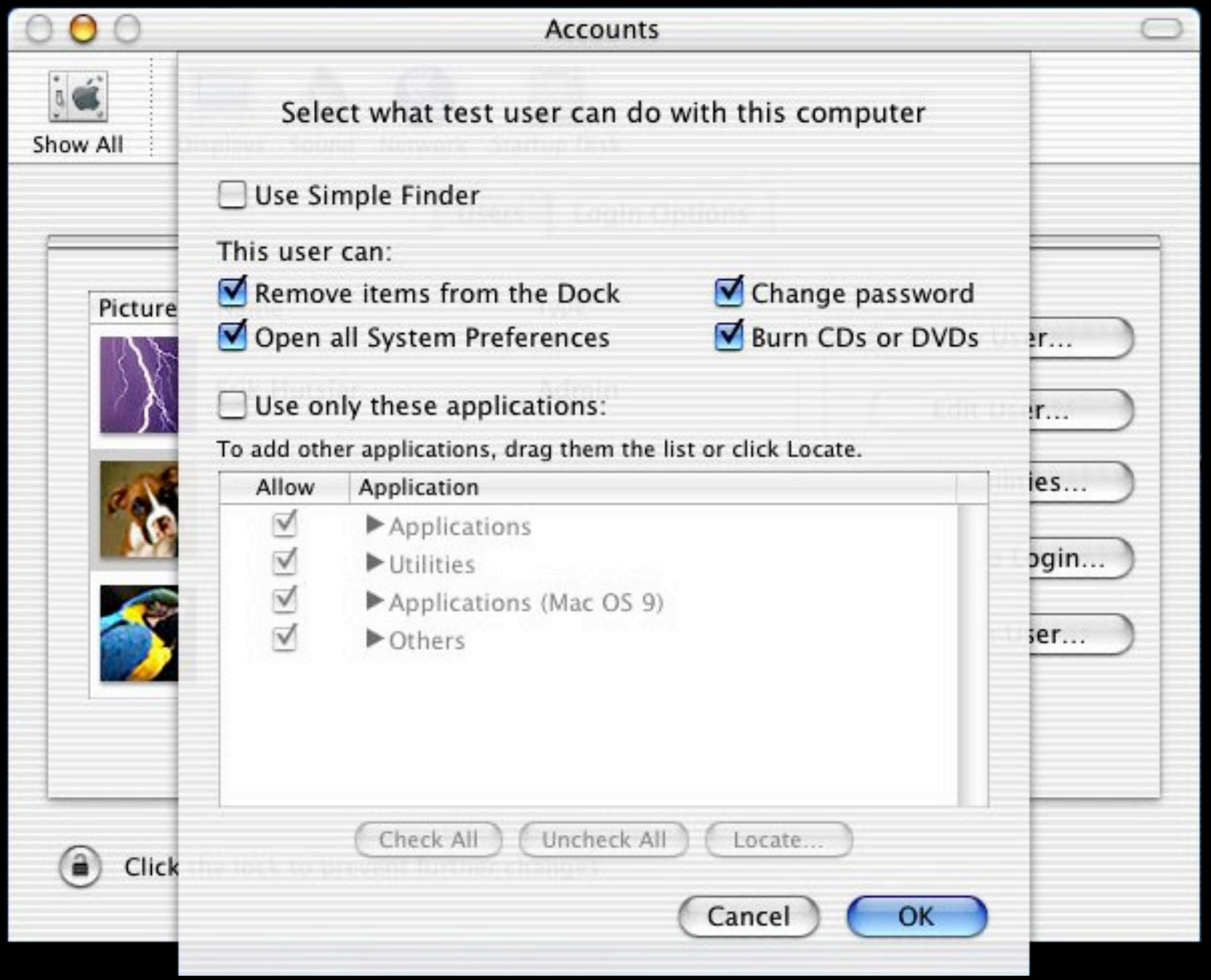
- Authorization controls
- Authentication services
- Cryptographic services
- Certificate handling

Authorization Controls

- Desktop user access control
- User manager integrated into Mac OS X
- Work Group manager integrated into Mac OS X server

User Management

Local user capabilities



Authentication and Directory Services

Authentication Services

- Open Directory
- Password Server
- Kerberos

Enterprise Integration

Integrate with your existing network infrastructure

- Open Directory architecture enables integration with existing directory services
- Support for LDAP, NIS, NetInfo, Active Directory, BSD configuration files

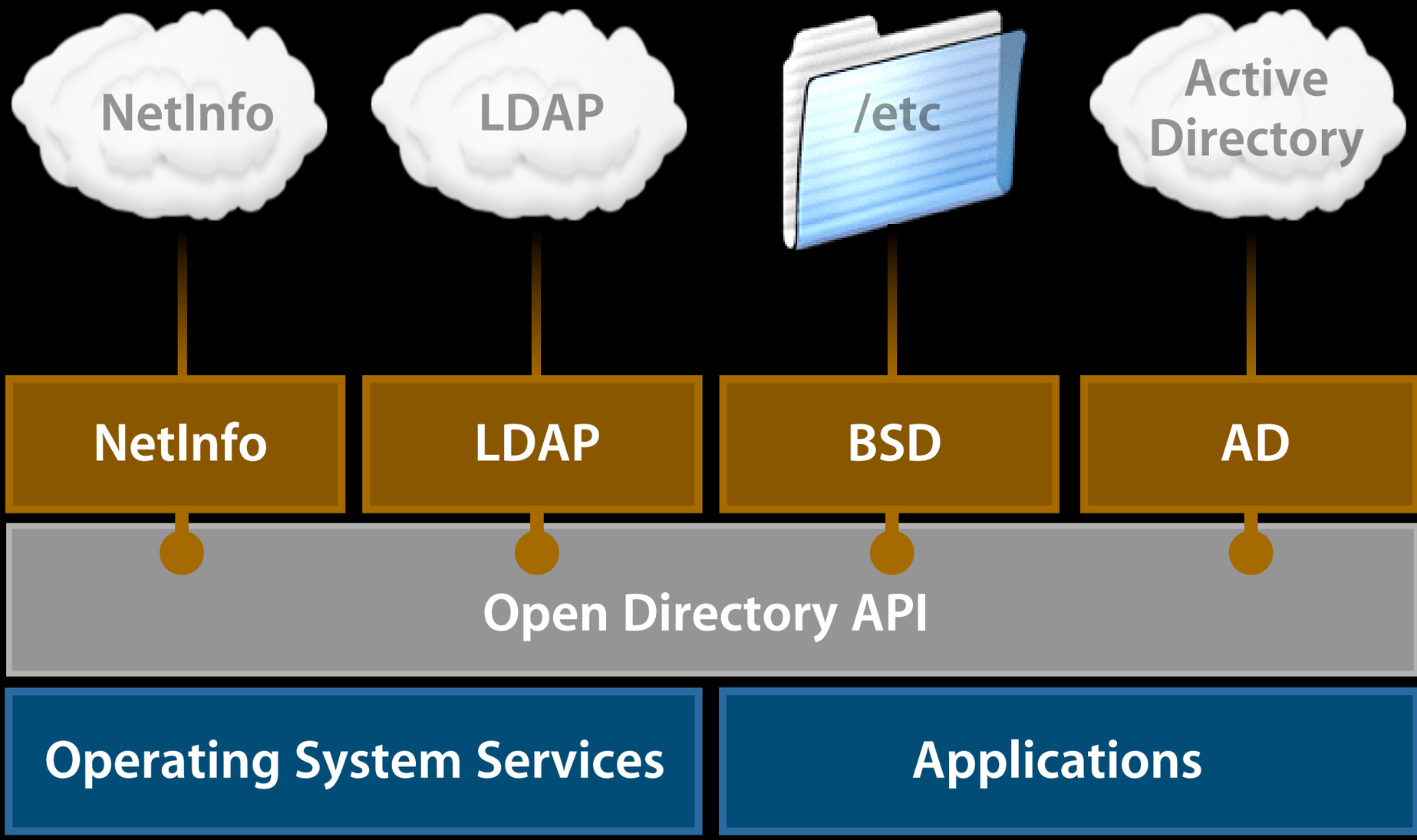
Open Directory Server

Easy to configure LDAPv3 directory server

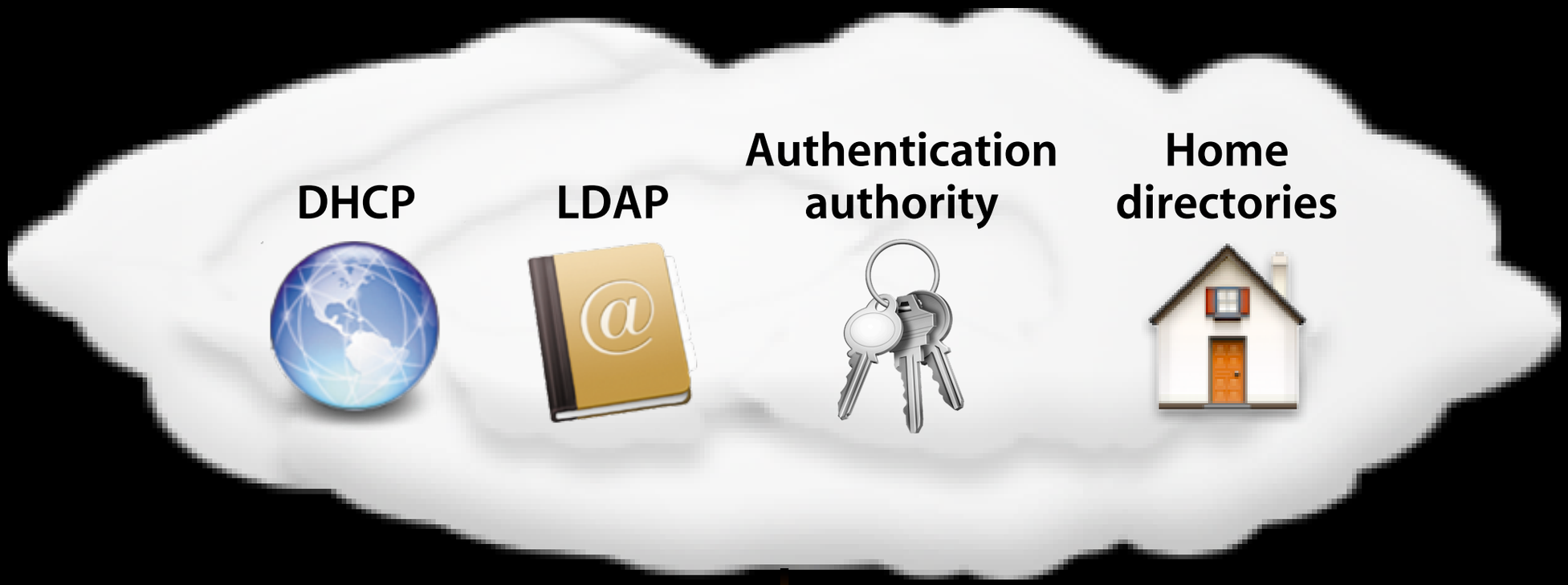
- Built-in LDAPv3 server with SSL security
- Easy-to-use setup assistant
- Based on OpenLDAP

Open Directory Architecture

Built-in support for directory services



Open Directory



Open Directory Authentication Standards-based Network Authentication

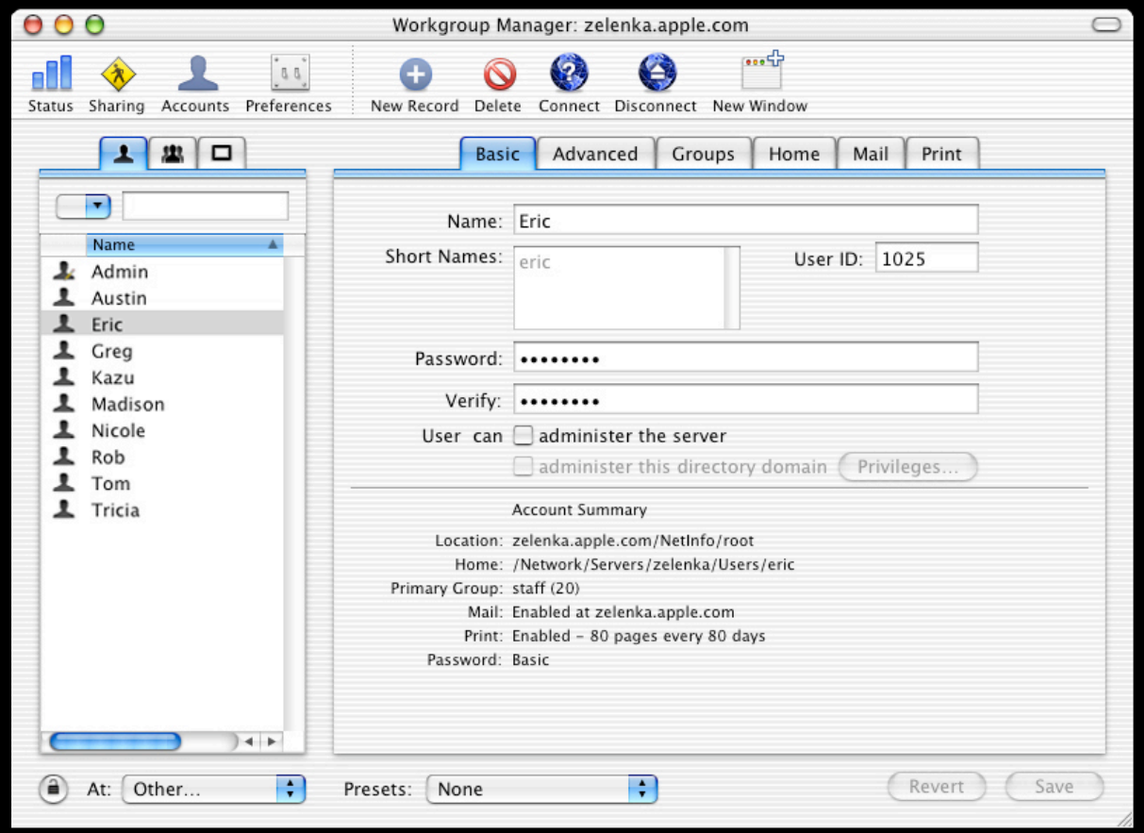
- Secure network-based authentication services using SASL (Simple Authentication and Security Layer)
- Password policy enforcement
  - Minimum character length
  - Password expiration
  - Disable inactive accounts
- Support for single user login—one password, different authentication methods

Kerberos

- Standards based
  - MIT v4 and v5
  - Single sign-on
  - Kerberized applications
    - Mail
    - FTP
    - Telnet
    - AFP
    - SMB??

Workgroup Manager

- Mac OS X server directory-based management tools
  - Manage users, groups, and computers from the network
  - Control access to software, hardware, and network resources
  - Manage system preferences on Mac OS X desktop and portable computers
  - Store directory information in any LDAPv3 server

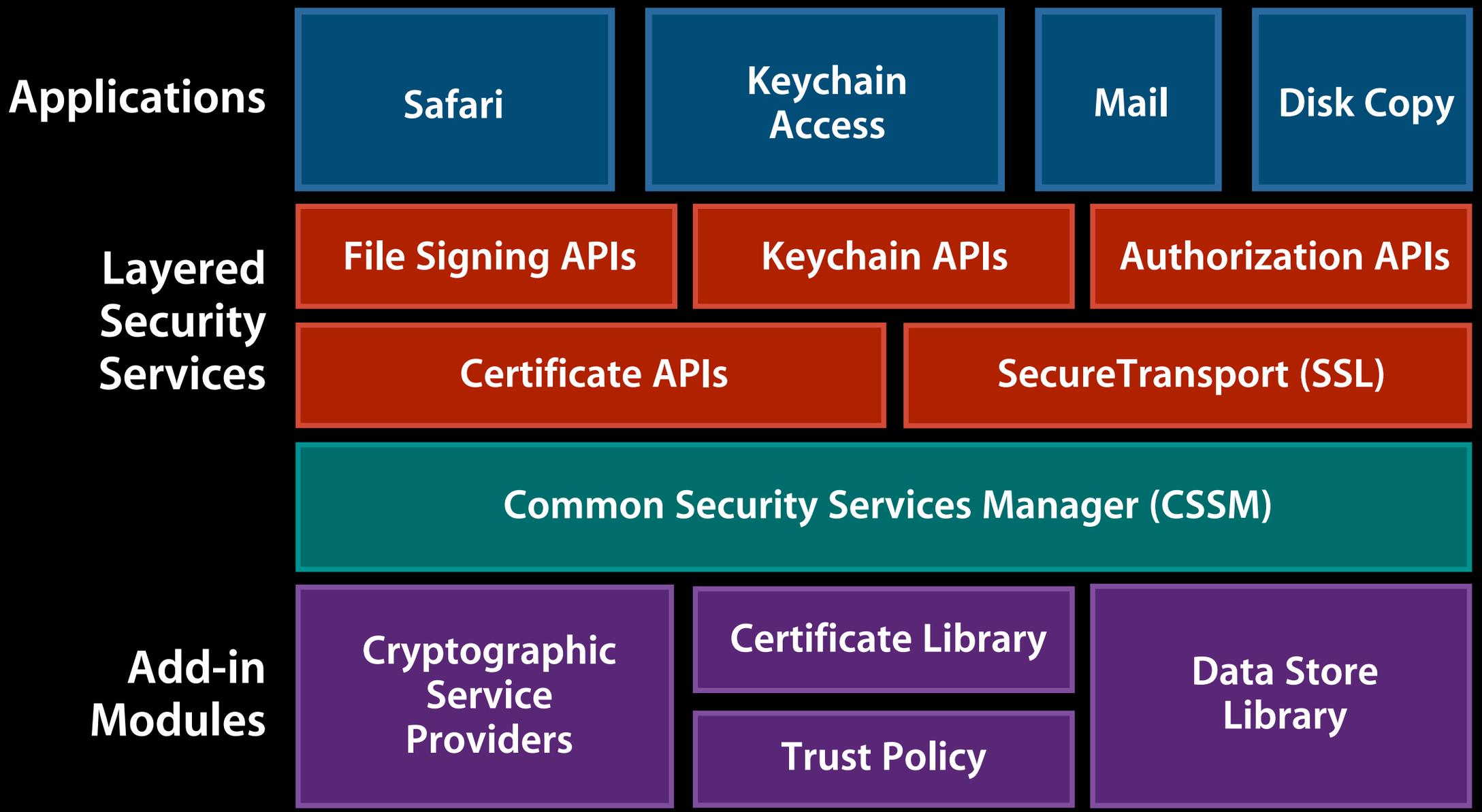


Security Services

Common Data Security Architecture

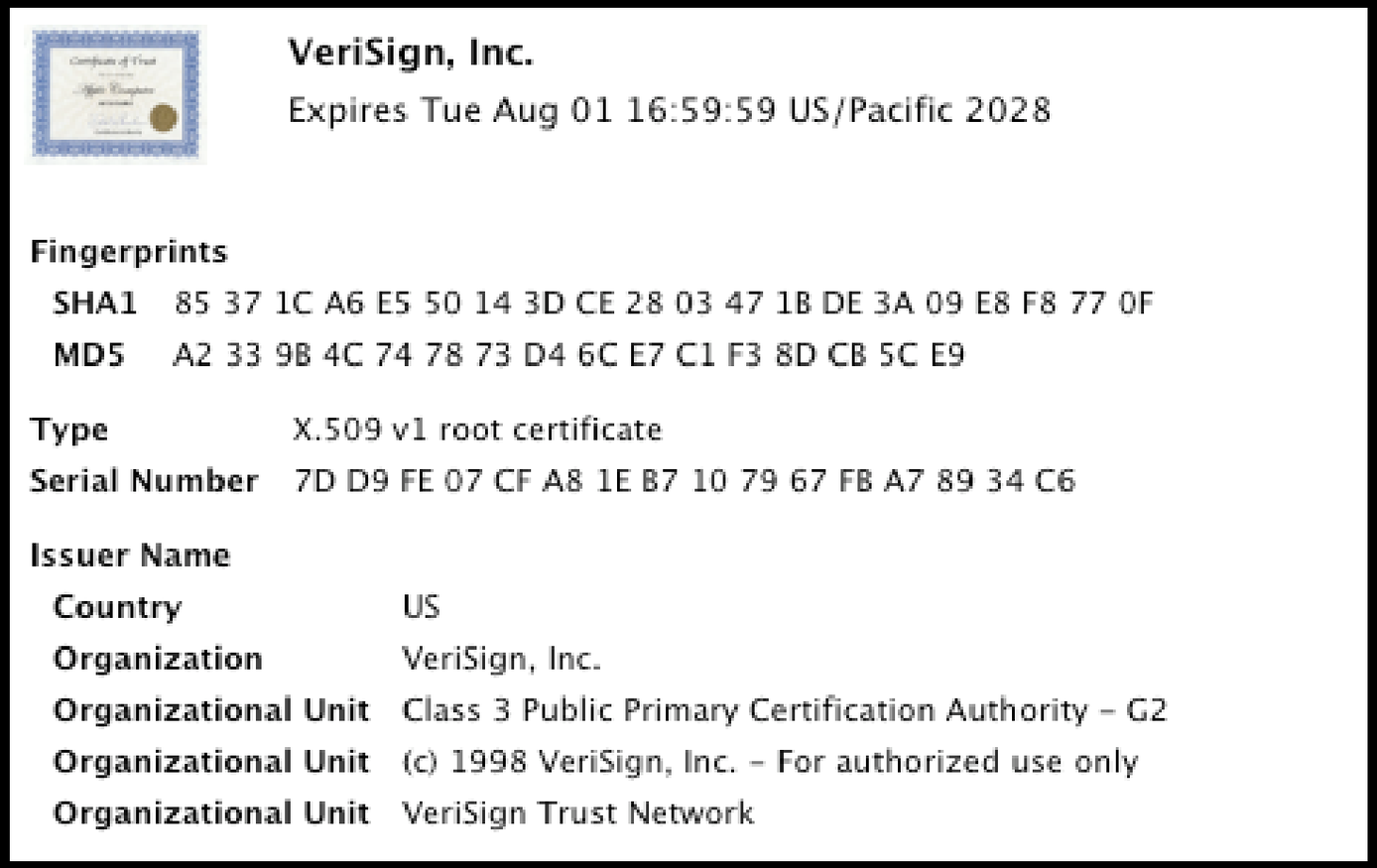
- Security core of Mac OS X
  - Layer set of security services
  - Plug-in security modules with common API
  - Customizable and extensible
  - Open source
  - Consistent set of security services
    - Developers
    - Apple

Common Data Security Architecture (CDSA)



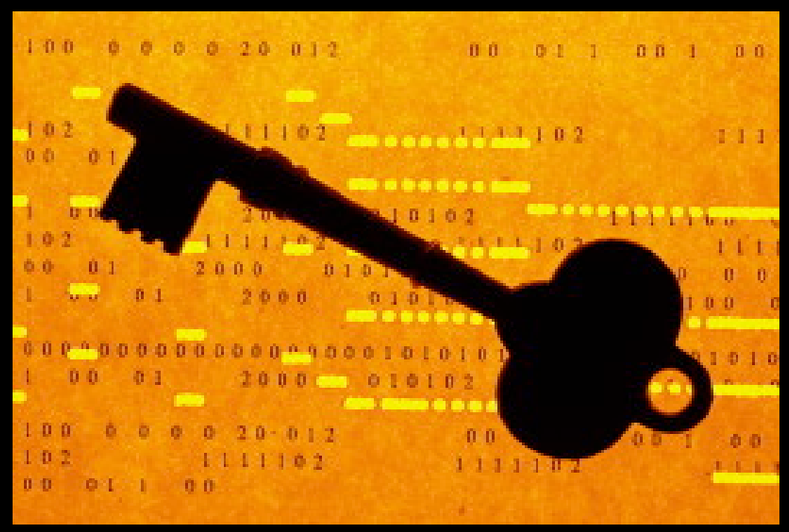
Certificate Handling

- x.509
- Enrollment–PKCS #7 and #10
- Issuance–PKCS #12
- Revocation–CRLs
- Verification–Trust Policy and Domains



Cryptographic Services

- AES encryption
- Complete set of algorithms
  - DES
  - 3DES
  - AES
- Message digest/integrity
  - MD5
  - SHA1
- Public key support
  - RSA
  - Diffie-Hellman
- Extensible service

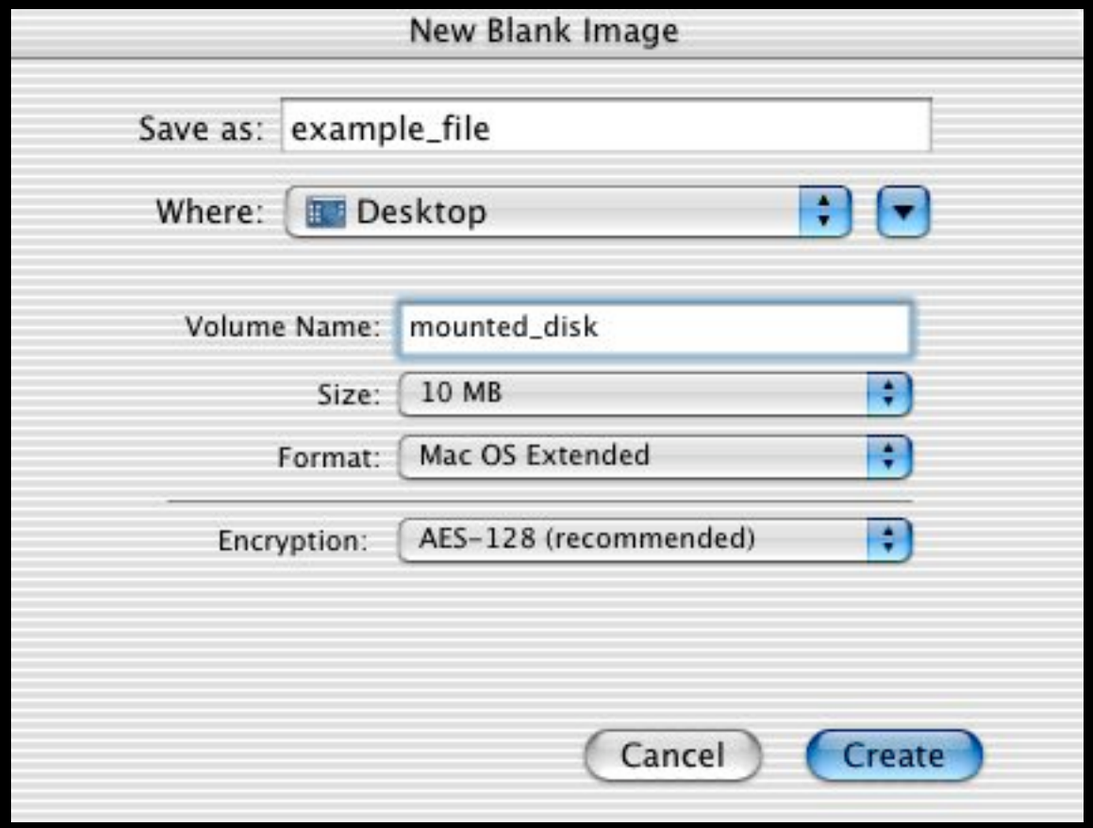


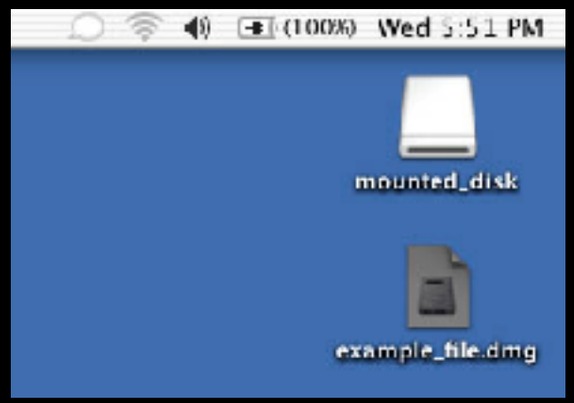
Encrypted Disk Images

- Data protection
  - AES 128-bit encryption
  - Appear like any other volume
  - High performance
  - Encrypt and decrypt “on-the-fly”

Encrypted Disk Images

- Easy-to-use





Keychain Access

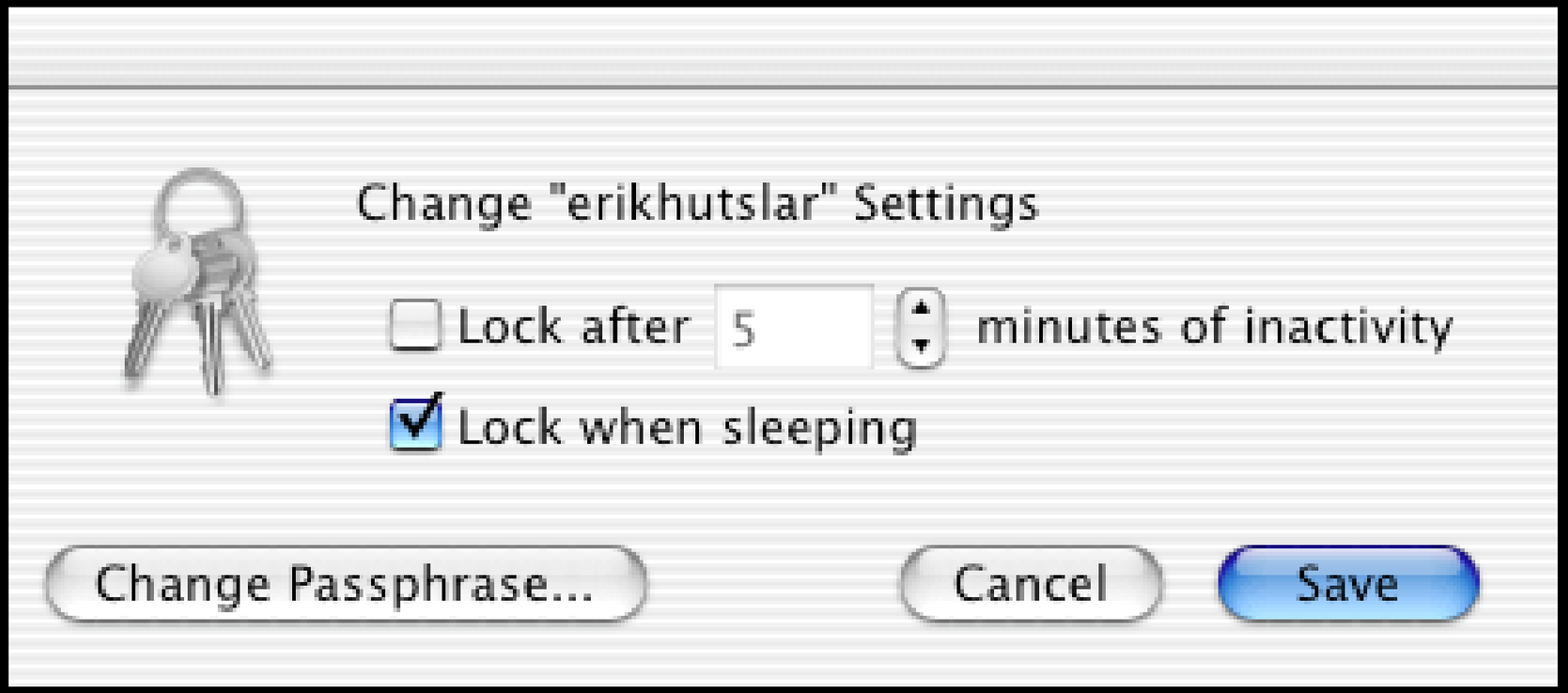
Password management

- Supports multiple users on one computer, each with a unique keychain
- Enables single sign-on with the log in password
- Stores information locally, not on a web server
- Supports long keychain passwords
- Stores other information securely
- ATM and credit card PINs
- Web server passwords
- Notes

Keychain Practices

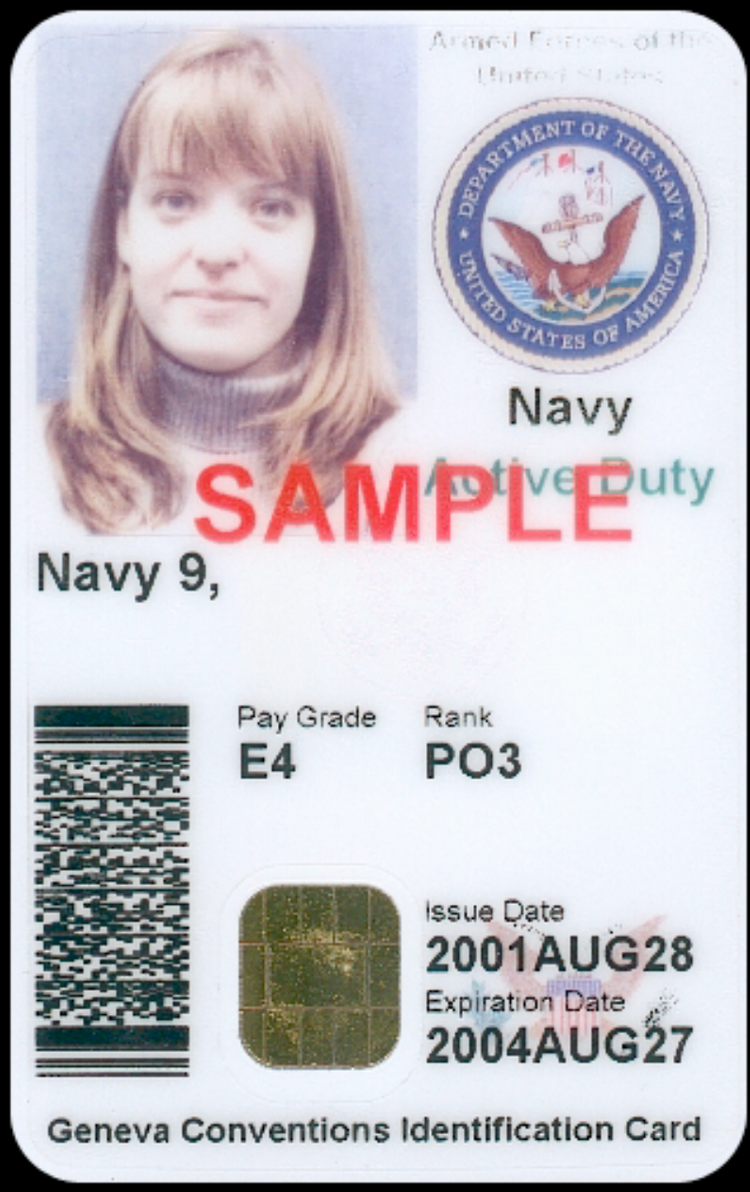
Increase security

- Set timeout for Keychain lock
- Set lock on Sleep
- Create a second Keychain for super sensitive passwords
- Store Keychain on removable device



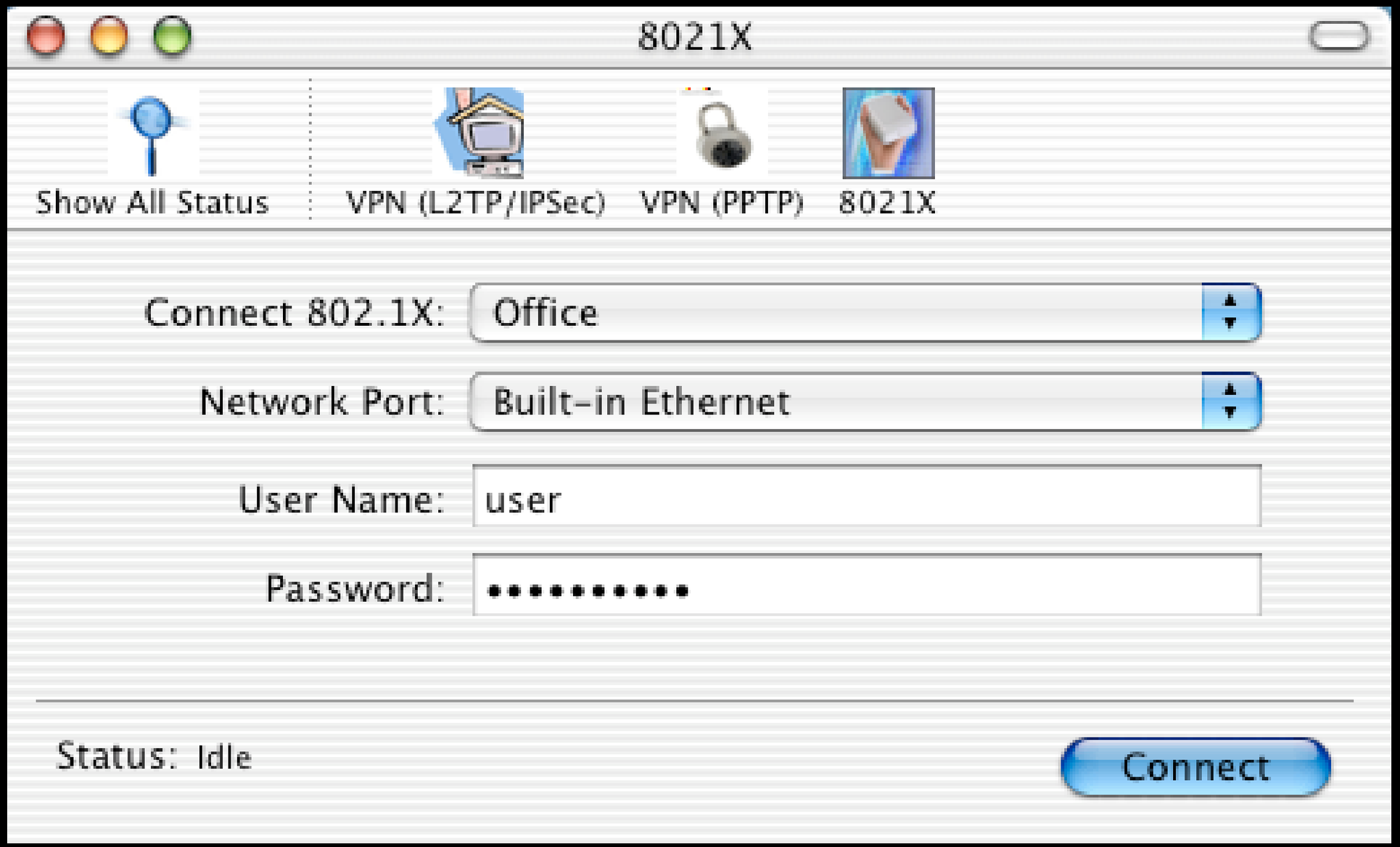
DoD Common Access Card

- Support now in Panther
  - Contains 3 certificates
    - Encryption
    - Identity
    - Signing
  - Java Applet on card
  - ReadCAC application
  - Authentication for
    - Login
    - Screen saver
    - System settings

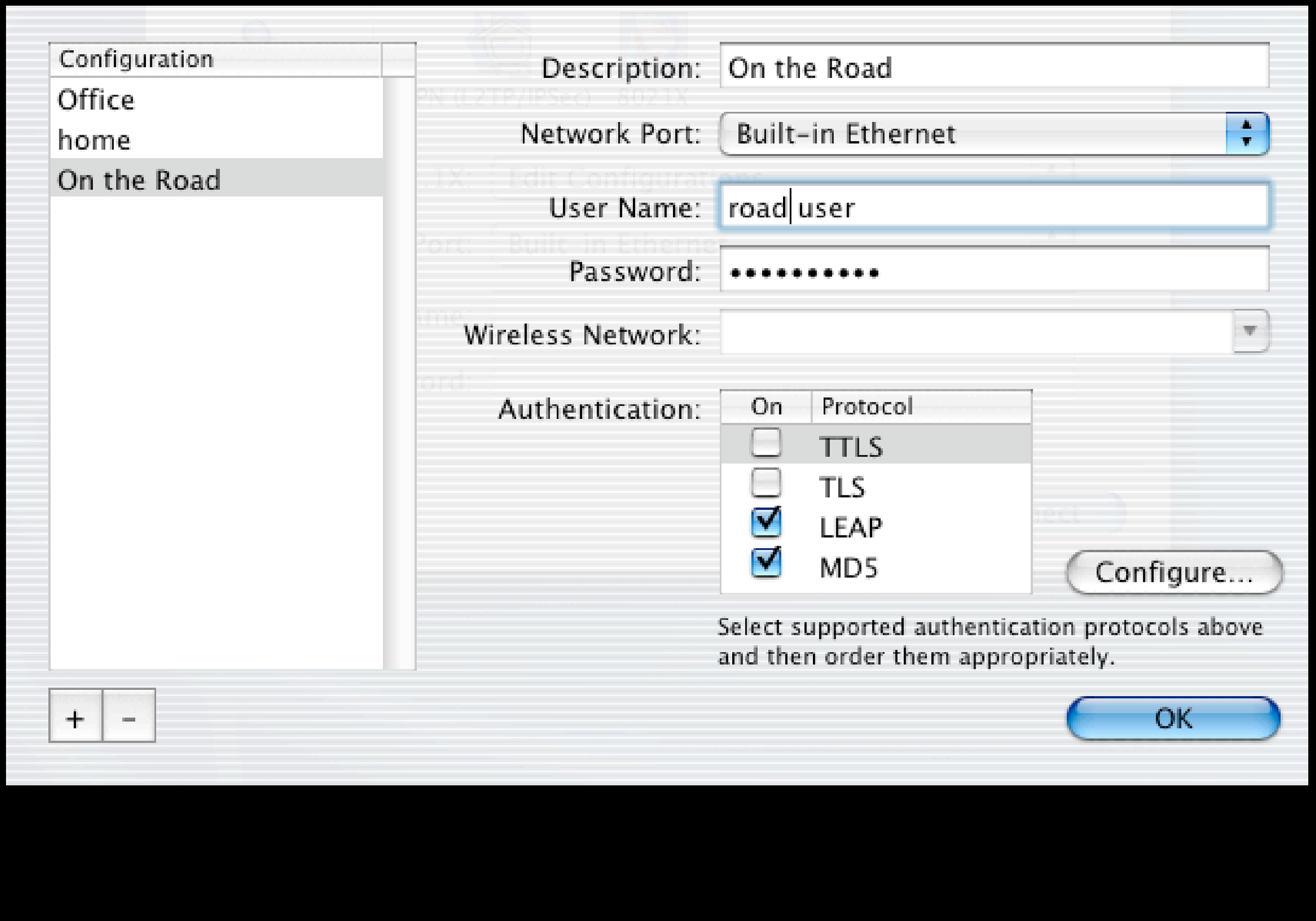


Network Security

Secure Connectivity

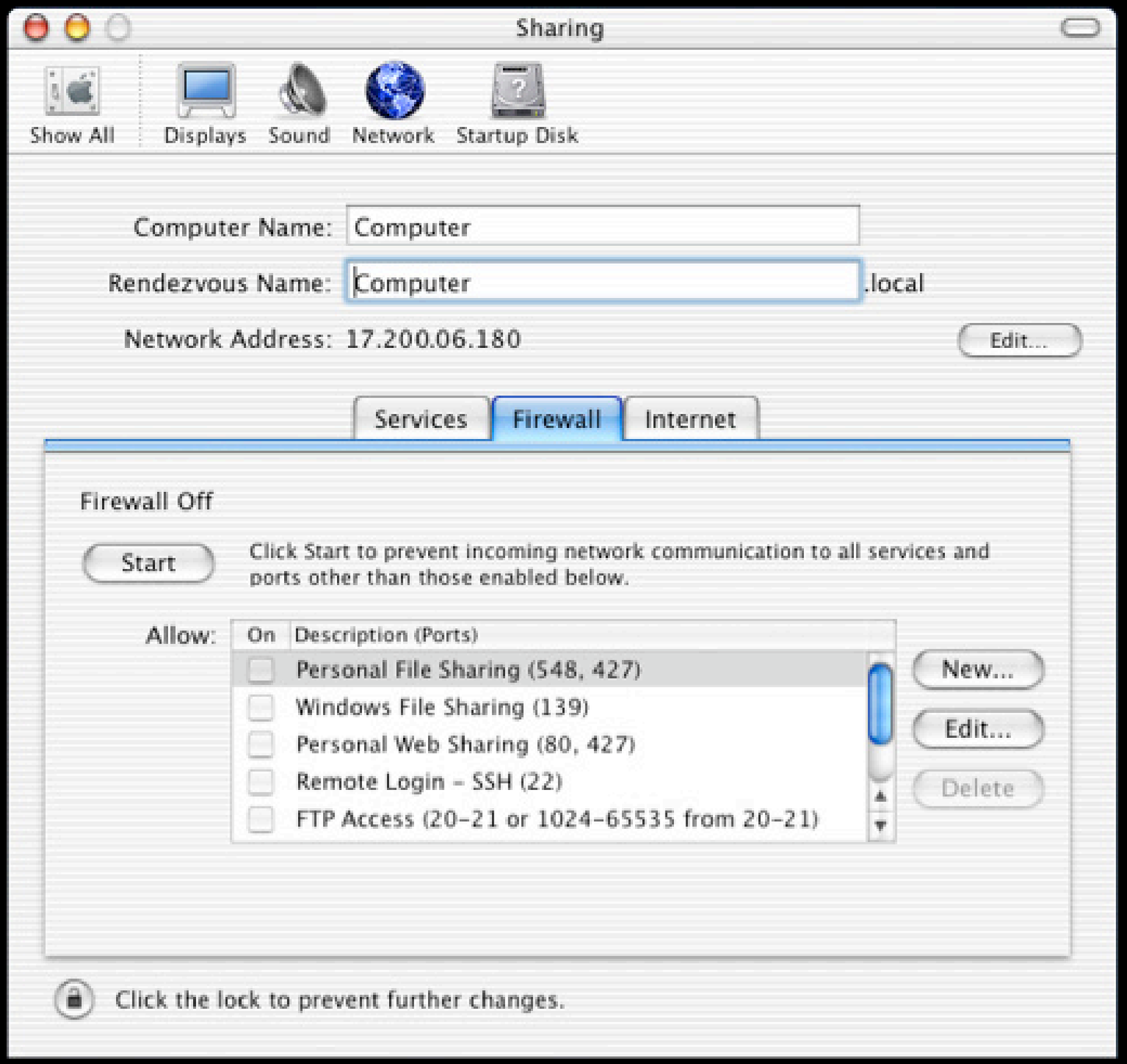


Multiple Configuration Support

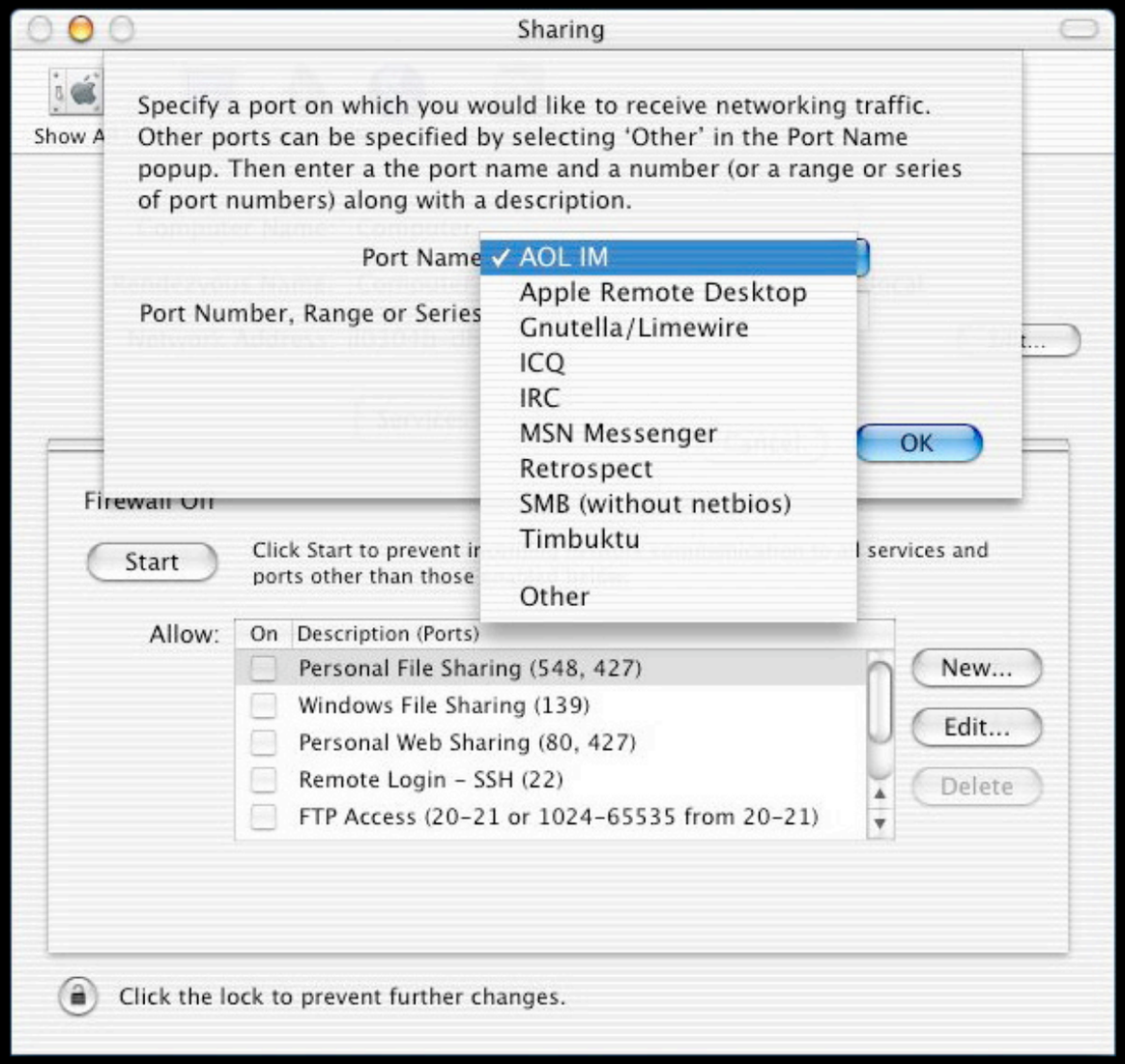


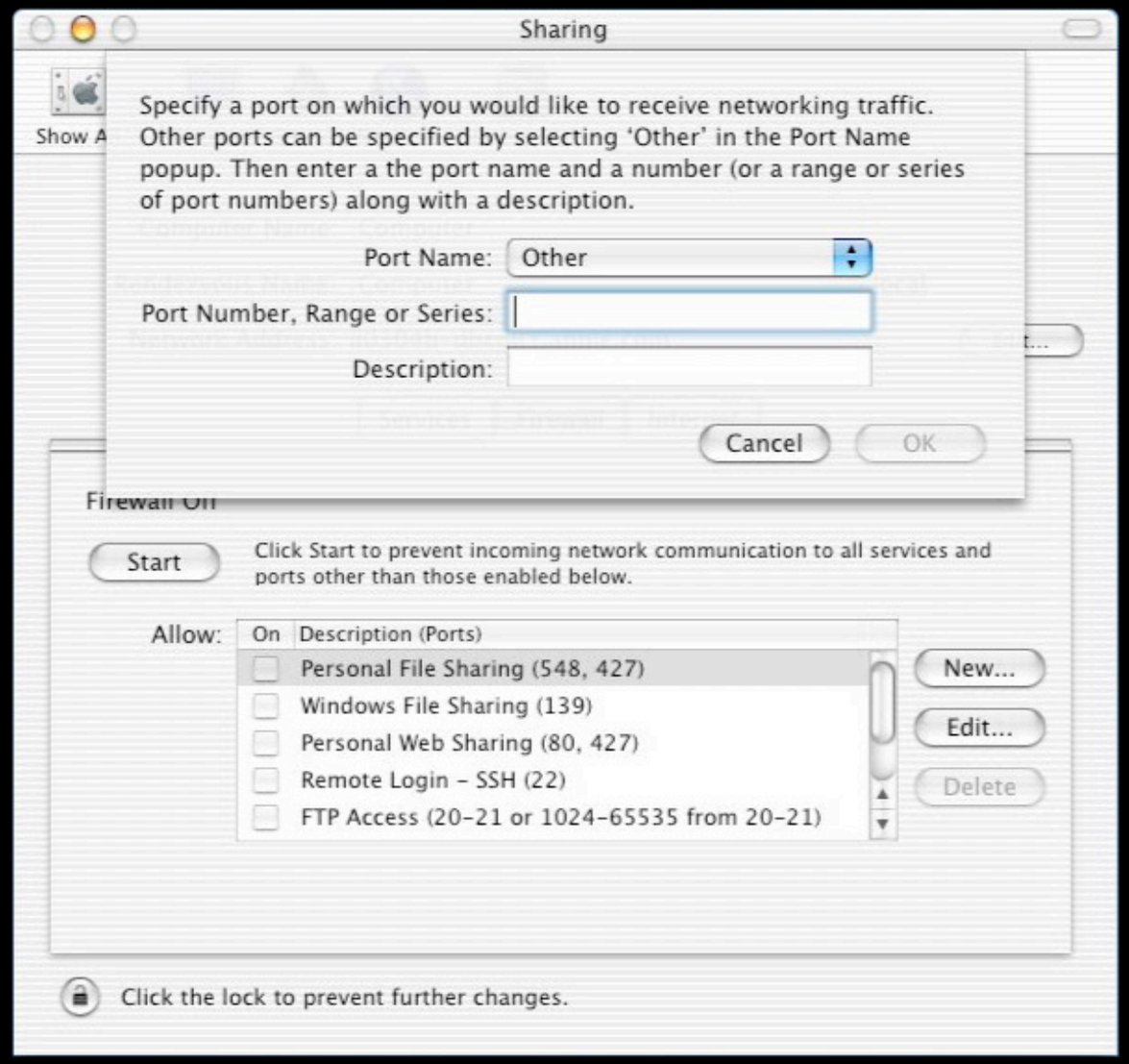
Built-in Firewall

Perimeter security using personal firewall



Customizable Firewall





Transport Security

- Secure communications
  - Secure Sockets Layer (OpenSSL v2/v3)
  - Transport Layer Security (TLS v1)
  - OpenSSH for secure command line access to systems

Security Communication

Stay informed

- Apple works with the community and external agencies, such as CERT and FIRST, to receive alerts to potential security issues in our products
- We host an external Security web site that provides basic security information, and a list of security-related software updates
- People can subscribe to the security-announce mailing list to receive security notifications from Apple
- Report a product security issue: product-security@apple.com

Security Updates

Always up-to-date

- Automatic notification for download and installation of security patches via the Software Update
- Updates digitally signed by Apple
  Industry leading response time

Recommendations

- Control physical access to resources
- Use Open Firmware Password Protection
- Take advantage of Encrypted Home Directories
- Securely erase files or folders
- Use the built-in Firewall
- Only turn on needed services
- Do not make everybody an administrator

Current and Future Initiatives of Mac OS X

Common Criteria Certification

Common Criteria

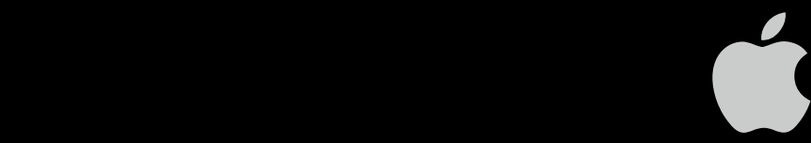
- Level playing field for security evaluations

Common Criteria Certification

- Level playing field for security evaluations
  - Independent certified lab evaluates vendor claims
  - Evaluates the security features and capabilities
  - Globally accepted ISO standard (ISO 15408)
  - Apple's targeted results?
    - Mac OS X and Mac OS X server certified [CAPP/EAL3]
      - Controlled Access Protection Profile—Functional requirements
      - Evaluation Assurance Level 3—Methodically tested and checked
  - Advantage for developers?
    - Certification of an Open Source kernel and frameworks
    - Secure foundation on which to build solutions

Current and Future Initiatives

- Security: Built-in, Not Bolted On!
  - [STOS] Secure Trusted OS Consortium
    - Community enhancing the Security of Darwin—**"SE-Darwin"**
  - DARPA: Defense Advanced Research Projects Agency
    - **CHATS:** Composable High Assurance Trusted Systems
  - CRADAs: Cooperative R&D Agreements
    - Trusted OS Collaboration
  - Federal **Smart Card** Integration
    - **DoD CAC:** Department of Defense Common Access Card
  - NIST–National Institute of Standards and Technology
    - FPKI-TWG, High-level API, Smart Cards, Security Frameworks



[STOS] Secure Trusted OS Consortium

Community development, enhancing the foundations

www.STOSDarwin.org

- Public, private, and academic
  - Collaborative Security Sandbox
  - Staging for Darwin to Mac OS X
  - Some completed projects:
    - Estimate on SE-Darwin "Level of Effort"
    - Apache mod_ssl over CDSA
  - Some active projects:
    - Mac OS X Security Guidance Documents
    - "SE-Darwin"

CRADA–Cooperative Research and Development Agreement

"Security Focused Research"

Benefits to Apple and collaborative partner?

- Technology Transfer enhances OS Security services
- Sharing of technical expertise, ideas, and information
- Enables partners to optimize resources

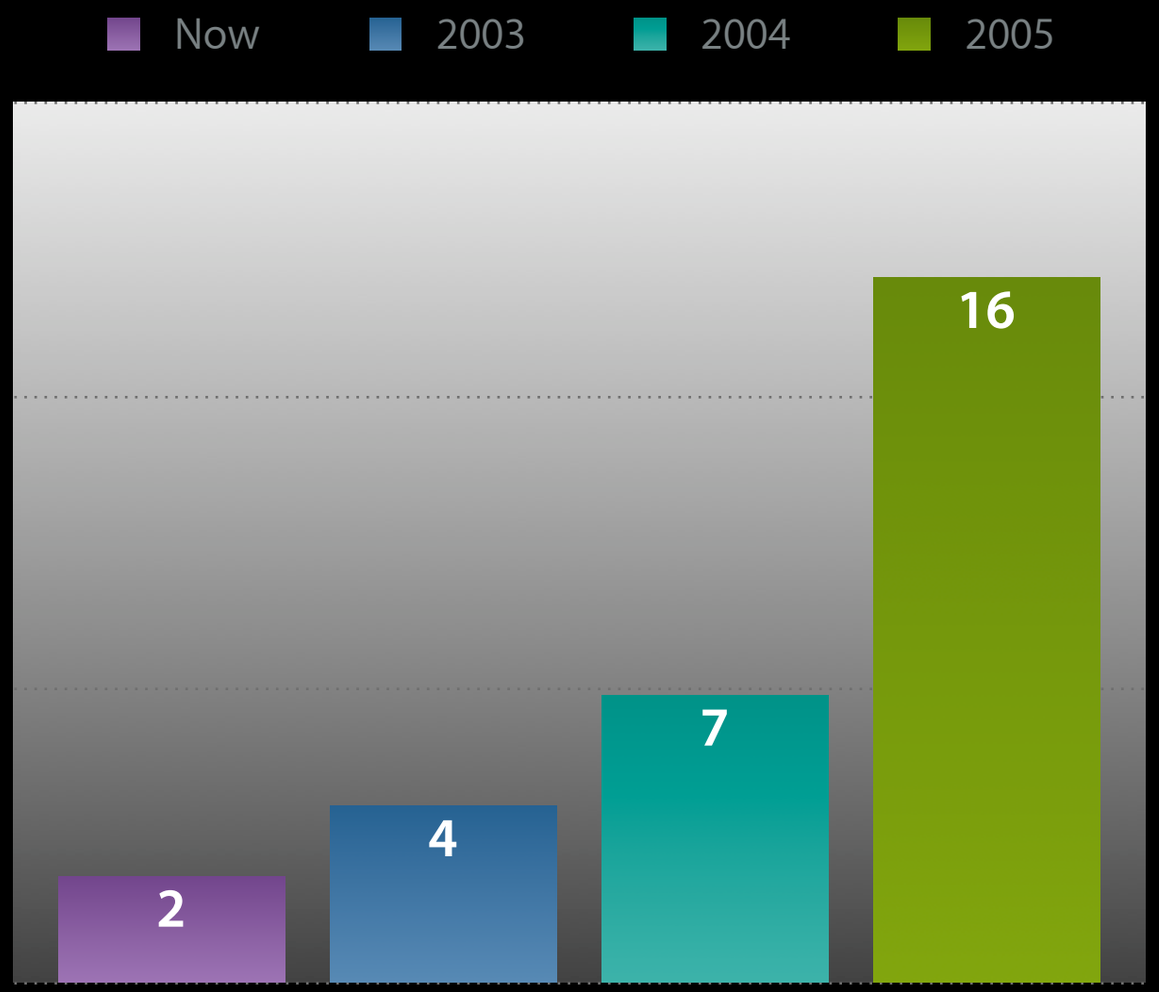
Benefits to Apple developers?

- Security Enhanced foundation to build solutions on
- Technology Transfer without engineering costs
- Can focus on developing your Killer Application

We all benefit!

Smart Card Integration

Massive deployment of digital identities



Anticipated # Deployed (in millions)

- DoD Common Access Cards
  - Multi-purpose ID
  - Issuing 10,000 daily
  - Will issue ~1.3 Million per year
  - Hopes to add Biometrics in 2004

Reference Library

Documentation

Security
Specifications and SDKs for Developers

http://developer.apple.com/macos/security.html

CDSA 2.0
Specifications

http://www.opengroup.org

Mac OS X Security

http://www.apple.com/macosx/technologies/security.html

Open Source
Apple's Open Source Repository

http://opensource.apple.com/

Reference Library

Documentation (continued)

Product Security
Apple's security information and reporting page
http://support.apple.com/security

[STOS] Secure Trusted OS Consortium
Open Collaboration on enhancing Security of Darwin
http://www.STOSDarwin.org/

Common Criteria
International Common Criteria Support Environment
http://www.commoncriteria.org/

Reference Library

Documentation (continued)

NIAP (NIST and NSA)
National Information Assurance Partnership

http://niap.nist.gov/niap/

Apple's Common Criteria efforts
What Apple is doing for Evaluation

http://www.info.apple.com/usen/security/index.html

NIST–PKI
High-Level API for PKI

http://csrc.nist.gov/pki/pkiapi/api.pdf

Q&A

Network Security

Best Practices for Mac OS X

http://developer.apple.com/wwdc2003/urls.html

WWDC 2003

Worldwide Developers Conference